Investigadores en ciberseguridad han expuesto una nueva campaña que probablemente ha tenido como objetivo los sectores automotriz y de comercio electrónico en Rusia, mediante un malware en .NET no documentado previamente, al que se le ha denominado *CAPI Backdoor*.

Según el laboratorio de análisis Seqrite Labs, la cadena de ataque inicia con el envío de correos de phishing que contienen un archivo ZIP, el cual sirve como vector para iniciar la infección. El análisis por parte de la firma de ciberseguridad se basa en un archivo ZIP que fue subido a la plataforma VirusTotal el 3 de octubre de 2025.

Dentro del archivo comprimido se encuentra un documento señuelo en idioma ruso, que aparenta ser una notificación relacionada con la legislación sobre el impuesto sobre la renta, así como un archivo de acceso directo de Windows (LNK).

Este archivo LNK, que lleva el mismo nombre que el archivo ZIP (es decir, *«Перерасчет заработной платы 01.10.2025»*), es el encargado de ejecutar el implante en .NET (*«adobe.dll»*) mediante el uso de un binario legítimo de Microsoft llamado «*rundll32.exe*«. Esta técnica, conocida como *living-off-the-land* (LotL), es comúnmente empleada por actores maliciosos.

Según indicó Seqrite, el *backdoor* incorpora funciones que permiten verificar si se ejecuta con privilegios de administrador, identificar los programas antivirus instalados en el sistema y abrir el documento señuelo como distracción, mientras establece una conexión oculta con un servidor remoto (*«91.223.75[.]96»*) desde el cual puede recibir nuevas instrucciones para ejecutar.

Las órdenes que puede recibir el *CAPI Backdoor* incluyen el robo de información de navegadores como Google Chrome, Microsoft Edge y Mozilla Firefox; la captura de pantallas; la recopilación de datos del sistema; la enumeración del contenido de carpetas; y la exfiltración de todos estos datos al servidor remoto.

Asimismo, el malware intenta llevar a cabo múltiples verificaciones para determinar si se

está ejecutando en un entorno real o en una máquina virtual, y emplea dos métodos para asegurar su permanencia en el sistema: la creación de una tarea programada y la generación de un archivo LNK en la carpeta de inicio de Windows, que lanza automáticamente la DLL maliciosa copiada en el directorio Roaming de Windows.

La evaluación de Seqrite sobre el posible enfoque hacia el sector automotriz ruso se basa en que uno de los dominios asociados con la campaña se denomina *carprlce[.]ru*, el cual parece estar suplantando al legítimo *«carprice[.]ru»*.

"La carga maliciosa es una DLL en .NET que actúa como herramienta de robo de información y establece mecanismos de persistencia para actividades maliciosas futuras", señalaron los investigadores *Priya Patel* y *Subhajeet Singha*.